

Remarks/Arguments

Claims 1-12 are pending. Claims 1, 7 and 10 have been amended to correct an obvious error and to more clearly and distinctly claim the subject matter that applicants regard as their invention. No new matter is believed to be added by the present amendment.

Objection to declaration

Responsive to the objection to the declaration filed on June 25, 2004, under 37 CFR 1.131, applicants hereby submit an English language translation of previously submitted exhibit A. Regarding the continuity of diligence leading up to the filing date of the application, applicants submit that applicants' documented performance of the steps leading to the filing of the application within a relatively short period of time sufficiently demonstrate applicants' diligence. In particular, the invention disclosure document was completed on October 6, 1998, the disclosure and declaration were signed pursuant to French law on October 14, 1998, the application was prepared and reviewed during October 14-19, 1998, and the application was filed on October 19, 1998. These steps were completed within 13 days. Applicants submit that the completion of the necessary steps within this short period of time sufficiently evidences applicants' diligence.

Rejection of claims 1-12 under 35 USC 102(b) as being anticipated by Söhne et al (US Pat. No. 6397333)

Even if Söhne is deemed to be valid prior art in the present application, Applicants submit that for the reasons discussed below present claims 1-12 are not anticipated under 35 USC 102(e) by Söhne.

The present invention relates to a copy protection method that includes the step of formatting the digital data from a source of digital data using a function based on at least a serial number contained in a medium, to thereby prevent bit by bit duplication of digital data onto another recording medium. Notably, the method provides for formatting the digital data using a function based on at least a serial number contained in the medium. The formatting of the digital data may be carried

out, for example, using a secret-key encryption algorithm such as DES or a public-key algorithm such as RSA, wherein the encryption key is dependent on the serial number. The formatted data is then stored on a medium. In this regard, present claim 1 recites:

formatting the digital data from said source of digital data using a function based on at least a serial number contained in said medium, to thereby prevent bit by bit duplication of the digital data onto another medium; and
recording said formatted data onto said medium.

and present claim 7 recites:

sending the serial number recorded on the medium to a reading device;
formatting the digital data read with the aid of the serial number, to thereby prevent bit by bit duplication of the digital data onto another medium; and
recording on said medium the formatted digital data.

Applicants submit that nowhere does Söhne disclose or suggest the cited features of claims 1 and 7.

Söhne discloses a system wherein the digital data is stored in the clear on the storage medium. In particular, Söhne et al. discloses (see col. 2, lines 42-57) a copy protection system and method in which a device having a unique identification (UID) sends the UID to a content provider supplying digital data. The content provider uses the UID to form an authentication signature of a digital data set (see col. 3, lines 30-55) and sends this signed data set (containing the digital data and the signature) to the device associated with the UID. The signed data set is copied in the device. The device checks the signature and releases the data set for read out upon successful checking of the signature (col. 3, lines 54-56). Then, when the data is to be read on a host, the device encodes the data set with the UID to form cipher data and sends the cipher data and the UID to the host (col. 3, lines 56-61; col 4, lines 65-67). The host then decodes the cipher data using the UID to restore and use the data in the host.

A notable difference between the method disclosed in Söhne and the method of present invention is that, in Söhne, the digital data set which is copied in

the device (i.e. in the medium) is not encoded or encrypted with the UID. It is only encoded / encrypted for transmission to a host. See e.g. col. 3, lines 62 where it is said, "the data set that is stored "straight" in the device... (emphasis added)" See also col. 4, line 64: "*The controller then writes the data set into a memory 6.*" In view of the specification of Söhne where the step of encoding / encrypting the data set using the UID is always recited after the step of storing / writing the data into a memory of the device / medium and in view of Fig. 1 where the "Encrypt" module is located at the output of the device, it is clear that the digital data is stored in the clear in the device / medium of Söhne. Consequently, if one hacker manages to access the memory of the device and makes a bit by bit duplication of the content of the memory, the hacker will obtain a copy of the clear data.

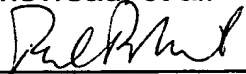
In view of the above, applicants submit that Söhne fails to disclose notable features of present claims 1 and 7, namely the formatting of the data and recording of the formatted data as recited in claims 1 and 7. Therefore, applicants submit that present claims 1 and 7, and the claims that depend therefrom, are not anticipated by Söhne.

Claim 11 recites the above-mentioned features of formatting the digital data in apparatus form, and is believed that claim 11 is not anticipated by Söhne for at least the same reasons as those discussed above with respect to claims 1 and 7.

Claim 12 recites a recording medium having digital data stored thereon, which is formatted in the manner discussed above, and as such, it is believed that claim 12 is not anticipated by Söhne for at least the same reasons as those discussed above with respect to claims 1 and 7.

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the applicant's attorney at (609) 734-6815, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully submitted,
Chevreau, et al.


By: Paul P. Kiel
Attorney for Applicants
Registration No. 40,677

THOMSON Licensing Inc.
PO Box 5312
Princeton, NJ 08543-5312

Date: 24 January 2005

CERTIFICATE OF MAILING

I hereby certify that this amendment is being deposited with the United States Postal Service as First Class Mail, postage prepaid, in an envelope addressed to Mail Stop AF, Commissioner for Patents, Alexandria, Virginia 22313-1450 on:

24 January 2005

Date


Eliza Buchalczyk